Defense Information Systems Agency
Department of Defense

Your Data in Transit:

Building Network Interoperability and Information Assurance Into Your Application's Data Communications

David Basel
DISA

SSTC, May 1, 2006

Agenda

- Why should you care?
  - David Basel, DISA, DoD PPS Manager
- What do you need to know?
  - Cragin Shelton, MITRE
- How do you use all this?
  - SMSgt Josh Walker, AFCA/EVPI

Why should you care?

- PPSM supports “baking security in”
- PPSM saves time and money when seeking C&A
- PPSM increases speed of system deployment in real world

BUT

Only if you include PPSM from the beginning of the SDLC

PPSM Goals

- Protect DoD Networks and Enclaves - Common Security Baseline
- DoD Interoperability
- Incorporation into Certification and Accreditation Process
- Incorporation into DoD Acquisition Process

Program Managers Benefits

- **Cost and Schedule**
- **Reduce Re-engineering and development due to Installation Unique Requirements**

Interoperability Benefits

- Reduce operational startup time for deployed units
- Provide standard architectures, implementations and solutions
- Reduce initial cost/eliminate fielding rework cost
- Cleanup legacy practices
- Reduce cross component conflicts (DFAS/DLA/Medical)

Vulnerability Management Benefits

- Identify existing vulnerabilities
- Prioritize remediation efforts (Fix the problems Identified)
- Advance notice of specific vulnerabilities
- Potential attack vectors known before exploits exist
- Immediate impact analysis during attack/protection decision

Communications Bandwidth Benefits

- Reduce Hostile/Unintended Traffic
- Effective bandwidth utilization

What Do You Need to Know?

- **What aspects of your system relate to PPSM requirements?**
  - **Cragin Shelton, CISSP**
  - **The MITRE Corporation**

What Do You Need to Know?

- **What kind of network traffic are you creating?**
  - **Is it OK to use?**
  - **Is it being used correctly?**
- **Where does that traffic go?**

What Kind of Traffic?

- Internet **Protocol**
- Application **Service**
- **Port**

==========

- SSTC 2005
- Crosstalk May 2005

Evaluating Traffic Types

- Is it OK to use?
  - PPS Category Assignments List (CAL)
    - Understand the Color Code
- Is it being used correctly?
  - Vulnerability Assessment Reports
    - Known or foreseeable problems
    - Configuration Guidelines
    - Mitigation Steps

Where Does That Traffic Go?

- Which networks are the computers on?
- Which network boundaries does the traffic cross?

How Many Networks?

- NIPRNet
- SIPRNet
- NMCI
- Hill AFB
- DREN
- 9th Air Force
- Post Medical Center LAN
- DECC DMZ
- Internet
- Boeing
- Lockheed Martin
- State Department
- Homeland Security
- et cetera

Network Types

- External Network
- DoD Network
- DoD DMZ
- DoD Enclave
- Enclave DMZ

Network Boundaries

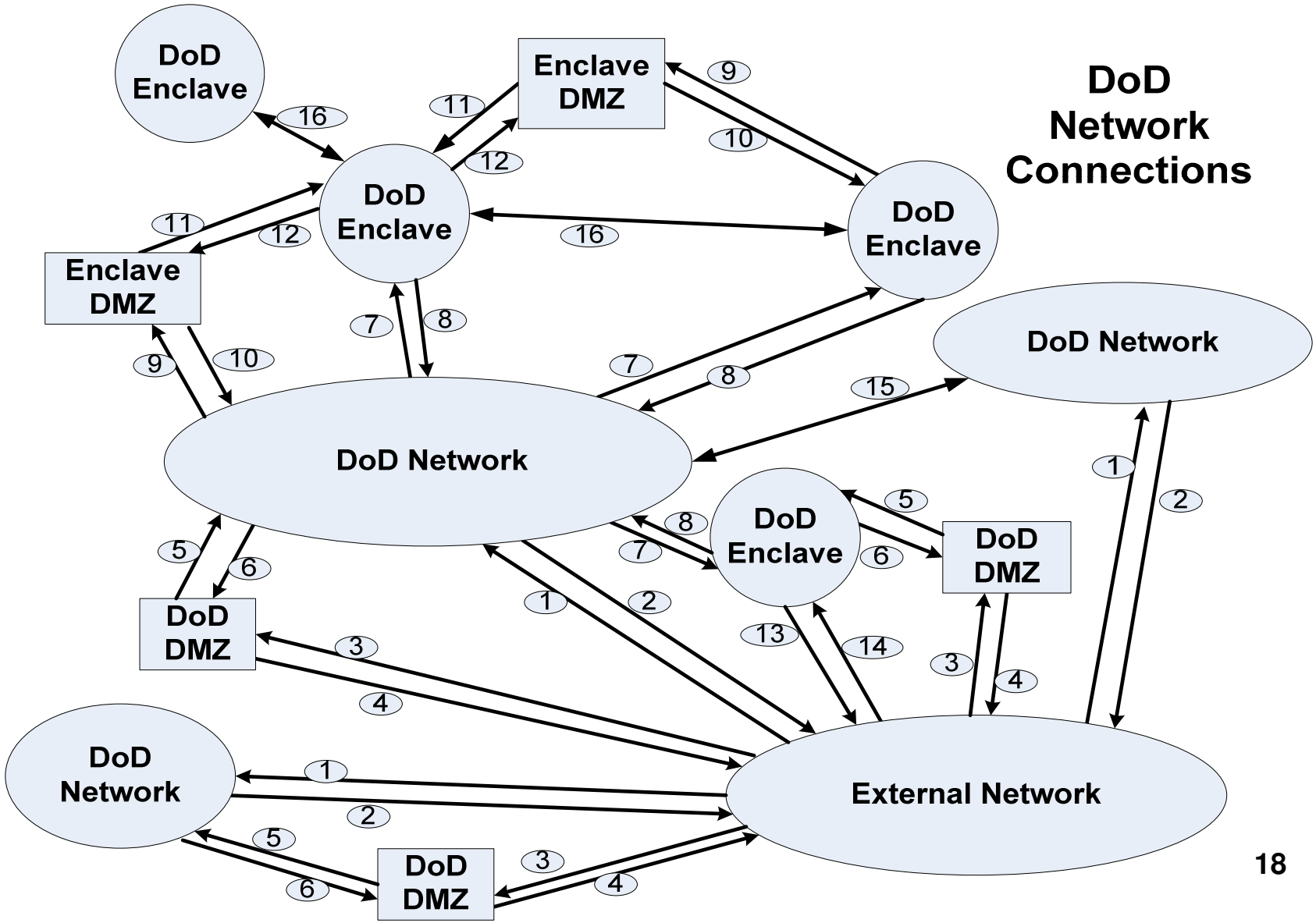
- Where networks connect
- Where security rules change
- Where security authorities change
- Where rules are enforced (firewalls)

  Direction matters

Boundary Crossings

1. External → DoD Network
2. DoD Network → External
3. External → DoD DMZ
4. DoD DMZ → External
5. DoD DMZ → DoD Network
6. DoD Network → DoD DMZ
7. DoD Network → DoD Enclave
8. DoD Enclave → DoD Network
9. DoD Network → Enclave DMZ
10. Enclave DMZ → DoD Network
11. Enclave DMZ → DoD Enclave
12. DoD Enclave → Enclave DMZ
13. DoD Enclave → External
14. External → DoD Enclave
15. DoD Network ↔ DoD Network
16. DoD Enclave ↔ DoD Enclave

Network Boundary Model



References

- DoD Instruction 8551.1
- PPS Assurance Category Assignments List (CAL)
- PPS Vulnerability Assessment Reports

==========

http://iase.disa.mil/ports

Definitions

- **Port**
  - Sub-address assigned to a program on a computer
  - One program may use one common port for listening, but separate, temporary ports for each specific conversation.
- **Protocol**
  - Generally, rules on format, order, and content for communication.
  - Specifically, rules to tell how to handle packets traveling on the Internet.
- **Service**
  - Particular rule set for how an application program communicates.
  - Also called Application Service, Data Service or Application Protocol

Acronyms

- **ACAL** — Assurance Category Assignments List
- **AFCA** — Air Force Communications Agency
- **C&A** — Certificatino & Accreditation
- **CAL** — Category Assignments List
- **DECC** — Defense Enterprise Computing Center
- **DFAS** — Defense Finance & Accounting Service
- **DITSCAP** — DoD Information Technology Security Certification and Accreditation Process
- **DLA** — Defense Logistics Agency
- **DMZ** — Demilitarized Zone
- **DREN** — Defense Research & Engineering Network
- **IP** — Internet Protocol
- **LAN** — Local Area Network
- **NIPRNet** — uNclassified IP Router Network
- **NMCI** — Navy / Marine Corps Intranet
- **PPSM** — Port, Protocol, & Service Management
- **SDLC** — System Development Life Cycle
- **SIPRNet** — Secret IP Router Network

www.disa.mil

How do you use all this

SMSgt Josh Walker
AFCA
SSTC, May 1, 2006

How do you use all this?

- **Perspective on integration and implementation of PPS by Air Force**
  - **SMSgt Josh Walker**
    AFCA/EVPI

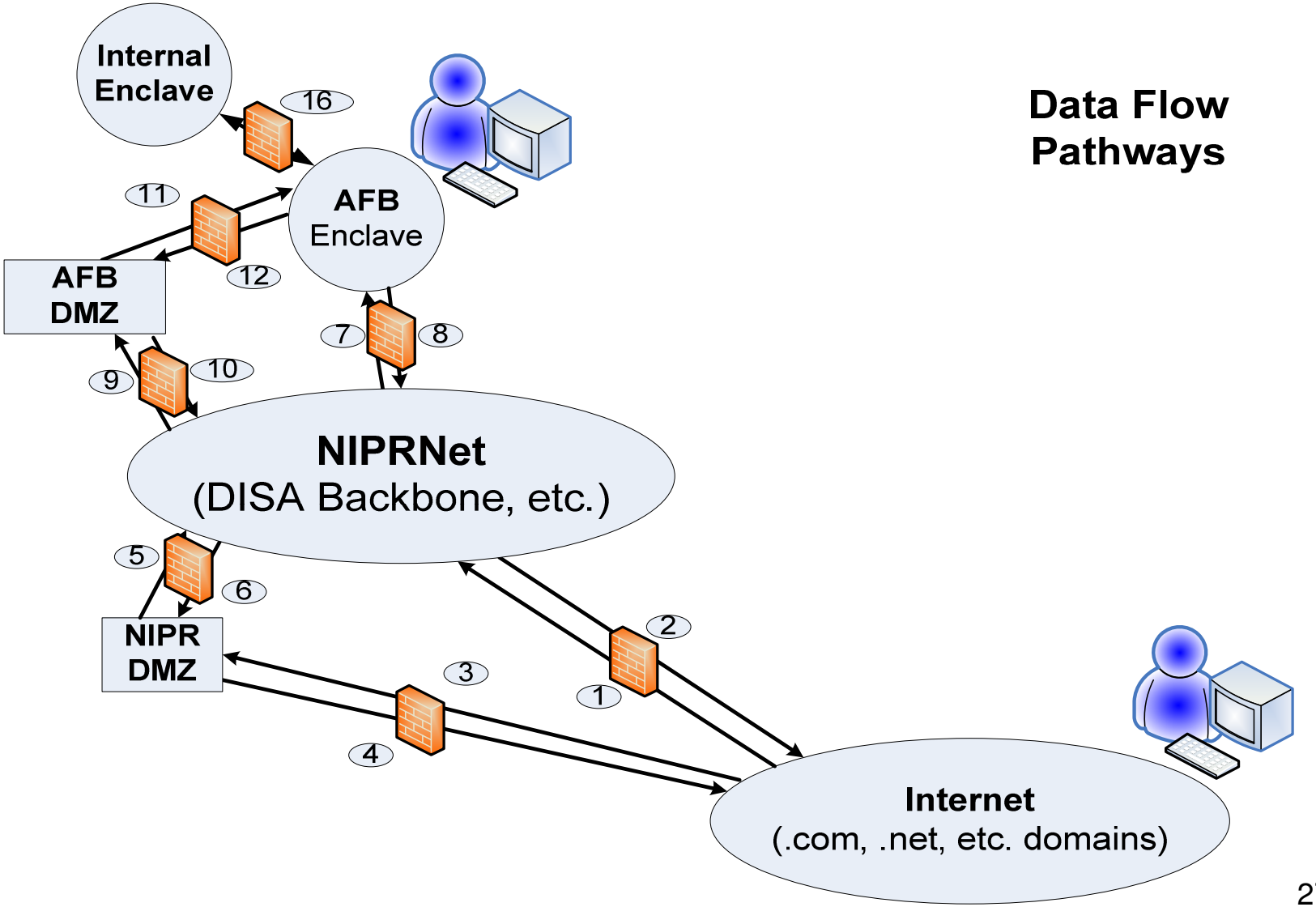
How do you use all this?

- During Design:
  - Use DoD ACAL to determine proper PPS to use based upon risk factors
  - Use PPS VA reports to determine “best practices” for configuration and use of PPS
  - Use “implementation guidelines” in your designs
- Make security a fore-thought instead of after-thought

Document, document…

- During Building and Testing:
  - Determine the overall system architecture (physical and logical)
  - All possible system interfaces at TCP/IP layer
  - Complete data flows at TCP/IP layer
- Determine your network boundaries
  - Overlay your system architecture onto “DoD Network Boundary Model”
  - Network boundaries all based upon source and destination (your system interfaces and data flows)

Example – Network Connections



Approval and Registration

- **Prior to Release:**
  - **Integrate complete PPS information into DITSCAP* documentation**
  - **Receive approval thru C&A or other service component/agency process**
  - **Register system PPS with DoD**
- **Impact of above:**
  - **Gives field "heads-up" on your system's deployment and impact to their enclave security**
  - **Approval and registration are necessary steps to allow your PPS across network boundaries**

***DITSCAP—DoD Information Technology Security Certification and Accreditation Process**

Implementation

- During Release and Support:
  - Maintain adherence to latest DoD PPS CAL risk designations and implementation guidelines
  - Do policy changes impact your system?
  - Are any system/network interface/data flow changes necessary?
  - All part of continuing risk management and C&A process
- Problems?
  - Proper approval will show how your PPS vulnerabilities were addressed and mitigated
  - Proper registration will give DoD visibility into PPS necessary for your system operation

Air Force References

- **AF Instruction 33-137, *Ports, Protocols and Services Management***
- **AF PPS Matrix**
- **AF PPS Management Documentation Guide**
  - **"AF-DoD PPS Worksheet"**

==========

https://private.afca.af.mil/afcaia/info_services/compusec_sec.cfm?COMPID=11

public.afca.af.mil